LECTURE 17.

ALIREZA SALEHI GOLSEFIDY

1. Irreducibility test.

Last time we were in the middle of the following question:

Is $x^5 - 2x^2 - x + 1$ irreducible over $\mathbb{F}_3$?

By checking its values, we can see that it has no zero in $\mathbb{F}_3$. So it has no degree 1 factor. How about degree 2 factors? It is easier if we check only irreducible monic degree 2 polynomials. But how can we find these polynomials? By excluding the reducible ones. Doing so, we get three monic irreducible degree 2 polynomials and after checking we see that $x^5 - 2x^2 - x + 1 = (x^2 + 1)(x^3 - x + 1)$, which means it is reducible.

Theorem 1. *Let $f \in \mathbb{Z}[x]$ and $\bar{f}$ be f modulo p. Assume $\deg(f) = \deg(\bar{f})$. If $\bar{f}$ is irreducible over $\mathbb{Z}/p\mathbb{Z}$, then f is also irreducible over $\mathbb{Q}$.*

We proved it in the class. Our proof is similar to the proof in your book.

Remark 2. The inverse is not necessarily correct. For instance $x^4 + 1$ is irreducible over $\mathbb{Q}$ but it is reducible over $\mathbb{Z}/\mathbb{Z}_p$ for any prime p.

Example 3. *Is $f(x) = x^3 - 3x - x + 32$ irreducible over $\mathbb{Q}$?*

Answer: *Yes, look at f modulo 3. We get $x^3 - x - 1$. Now it is easy to see that this has no zero in $\mathbb{Z}/3\mathbb{Z}$. Since it has degree 3, it is irreducible over $\mathbb{Z}/3\mathbb{Z}$. Hence $f(x)$ is irreducible over $\mathbb{Q}$.*

We also defined prime elements and showed that in an integral domain a is prime if and only if $\langle a \rangle$ is a non-zero prime ideal.

Mathematics Dept, University of California, San Diego, CA 92093-0112

E-mail address: golsefidy@ucsd.edu

Date: 2/22/2012.